Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 01, January -2018

Reputation Based Trust Mechnism to Isolate JellyFish Attackers in Mobile Ad Hoc Network

[1]Annu Kumari, [2]K.K. Joshi

[1]M.Tech Sudent ,Department of Computer Science and Engineering, MPCT, Gwalior, India
[2]H.O.D, Department of Computer Science and Engineering, MPCT, Gwalior, India

Abstract— *with the advancement in technology, Mobile Ad Hoc Network provide communication a number of the nodes for the movement of data from source to destination. In a MANET every tool is loose to transport independently in any route, and could consequently trade its links to other gadgets frequently. Each must forward traffic unrelated to its personal use, and it acts as a router. MANETs contains one or extra and specific transceivers among nodes. It is wireless medium which make it susceptible to various attacks. Jellyfish attack is mainly considered as common in the network in which packets are not reached towards the destination properly. In our proposed work, we used reputation based scheme for the removal of malicious nodes from the network and reduce the effect of Jellyfish attackers. We used NS2 for the simulation of our proposed work and show the difference between existing and proposed work in the network.*

Keywords*—MANET, JF Attack, Malicious nodes, Reordering packets, Dropping packets, Trust, Security and Protocols.*

I. INTRODUCTION

Among various wireless technologies, Mobile Ad hoc Network (MANET) is an active network in the communication. MANET is self-computing, dynamic and framework-less network. As in Fig. 1 over a wireless link its mobile nodes are related to each distinctive. At any immediate of time in MANET, any mobile node has the liberty to meander out of doors and within the network.

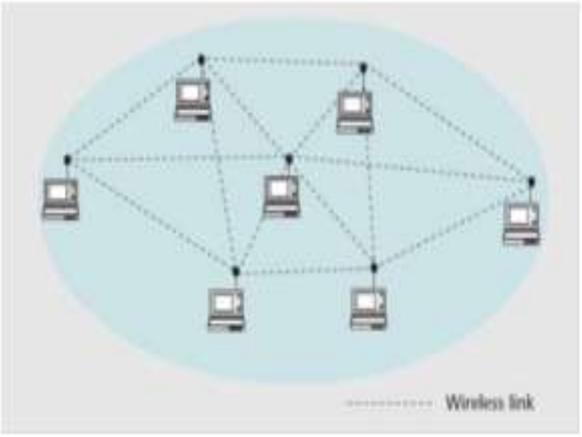

Fig.1 MANET Architecture

Minimum resource utility, Self-constructive, Distributive and cost consumption are some of the advantages of MANETs. The number one reason of MANET is to employ itself in a vital application inclusive of military scenarios, emergency motive, data networks, device networks and commercial sectors and so on. High performance is needed for MANET to handle the above vital application.

A MANET is a continuously self-configuring, infrastructure-a lot less network of mobile devices connected without wires. In a MANET every device is free to move independently in any course, and could therefore alternate its hyperlinks to different devices regularly. Each should forward traffic unrelated to its very own use, and it acts as a router. MANETs carries one or more and one-of-a-kind transceivers between nodes. MANETs include a peer-to-peer, self-forming, self-recuperation network. Typically they speak at the Radio Frequency between 30MHZ –5GHZ [1].

II. JELLYFISH ATTACKS

Jellyfish attacks might also additionally keep active in both course discovering and packet forwarding if you need to save you it from detection and diagnosis, however the malicious node can attack the traffic thru itself with the aid of way of reordering packets, dropping packets periodically, or growing jitters.The Jellyfish attack is in particular dangerous to TCP traffic in that cooperative nodes can hardly ever differentiate those attacks from the network congestion.

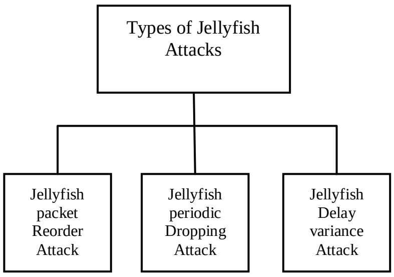
Types of Jellyfish Attacks
Jellyfish packet Reorder Attack
Jellyfish periodic Dropping Attack
Jellyfish Delay variance Attack

Fig.2 Types of Jellyfish attacks

As shown in Figure-2, node JF is a Jellyfish, and node S starts to speak with node D after a path through the Jellyfish node is mounted. Then the DoS attacks launched by using node JF will motive packet loss and damage off the communications between nodes S and D subsequently [2].

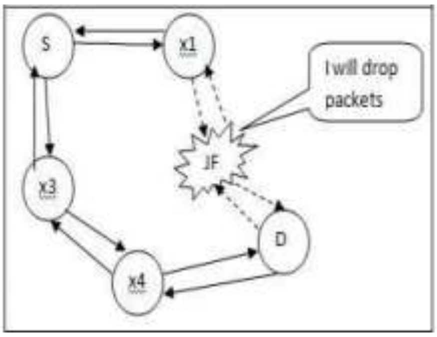

Fig.3 Jellyfish attack scenario

III. TRUST

a) What is Trust?

The belief of trust is significant to communication and network protocol designers where setting up agree with connections among taking part nodes is key to allowing synergistic improvement of framework measurements. According to Agarwal et al. [3], trust is described as “a set of members of the family amongst entities that participate in a protocol”.

These foundations depend on the declaration caused by utilizing the past collaborations of substances inside a protocol. In vast, if the interactions have been practical to the protocol, then trust will buildup among these nodes” Trust is outlined because the degree of belief concerning the mien of different entities.

b) Trust mechanism

Trust is introduced to save you from numerous attacks like worm-hole, black hole, Dos, Selfish attackers and so forth. Trust can be implemented in diverse methods along with recognition, subjective logic from opinion of needs and many others as there are no unique definition of accept as true with. According to accept as true with has following properties.

- Context Dependance : In some particular context accept as true with relationships are relevant
- Function of Uncertainty: Trust depends at the uncertainty of nodes motion. It gives the opportunity of motion executed by means of a node.
- Quantitative value: Trust can be assigned any type of numeric values discrete or non-stop.
- Asymmetric Relationship: Trust relationship is asymmetric in nature. In the event that node A trusts B and node B trust C that does not imply that A trusts C.

c) Trust and security

Trust and security should go hand in hand. The level of trust has an impact on the level of security. The wireless networks involve various types of security domains and security implementation mechanisms. A trust relationship which considers the heterogeneousness of these networks security procedures is essential. This can be accomplished by specifying the levels of security requirements and security mechanisms such as encryption, digital signature, authentication at the boundaries of each integrated networks. In other words, each of the integrated networks should contain their own security requirements along with the levels of trust (and even reputation) they are willing to provide to other networks or nodes [5].

IV. PROTOCOLS IN MANETS

Routing is a term that defines the course from source node to destination node. Routing in MANETs is more hard than routing in wired systems. In MANETs there are two sorts of routing: Table-driven routing and On- demand routing. Table- driven ad hoc routing protocols keep the routing statistics of each and every node connected to all other nodes within the network. Also referred to as proactive, these protocols allow every node to have a clean and consistent view of the network topology by way of transmitting updating messages periodically.

Another strategy is the source- initiated on- demand routing. According to this technique, a route is created simplest whilst the source node requires a direction to a specific destination. A route is acquired by using starting up the route discovery process through the source node. While route discovery, the data packets transmitted are supported and are sent when the course is set up. An mounted direction is maintained so long as it's miles required via a route maintenance manner. There isn't any routing protocol which is best for all types of MANETs. Each routing protocol has its own one of a kind qualities in a couple of particular networking situations, however mobile nodes should have the capacity to work in every environment. A challenge is a way to reap safety in routing as high as possible when it crosses over special environments.

- DSR
- AODV
- TORA [4]

V. LITERATURE SURVEY

R. Priyanka et al. [2016] on this work the conduct and effect of Jellyfish attack and Black hole attack over MANETs have been analyzed. Jellyfish attacks abuse the conduct of closed loop protocols alongside TCP, in this manner the location strategy moves toward becoming to hard. Subsequently the activity is upset prompting corruption in organize throughput.TCP has broadly perceived vulnerabilities to delay, drop and disorder the packets. The system presents a new consider primarily based detection algorithm that looks after jellyfish attacks in a MANET. This proposed algorithm is primarily based on trustworthiness of the nodes in network. Every node uses locally calculated accept as true with values which can be accrued over a time period to become aware of whether or not its neighbor node is a attacker or no longer. The attacker nodes observe the packets during the packet transmission and drop the packets before forwarding it to the destination [6].

Anjani Garg et al. [2016] in this paper, the main focus is to study and analyse the different techniques and systems proposed by the researchers in the literature in order to countermeasure the specific editions of JF attacks for MANETs. A JellyFish (JF) attack is particularly harmful against TCP-based mobile ad hoc networks (MANETs) where a malicious node exploits the behaviour of closed loop protocols such as TCP in order to delay, periodically drop or reorder the packets. This attack is carried out on the network layer, but it affects the performance of the transport layer protocol and causes severe degradation in end-to-end throughput in the network. The Jelly Fish attack is named a JF-Reorder attack, JF-Delay Variance attack and JF-Periodic Drop attack. JellyFish attack conforms to all present routing and forwarding protocol specifications, and consequently it will become very hard to discover [7].

Sakshi Sachdeva, et al. [2016] In this paper, we've connected Jellyfish delay variance attack on AODV and proposed a JFDV detection algorithm that analyzes packet delaying trouble making of nodes and detects more than one JFDV attacker nodes. It reduces common end-to-end delay and increase throughput via re-routing data packets through alternate route which includes non-malicious nodes [8].

Simranpreet Kaur et al. [2015] in this paper, a MANET is an adaptable and self configurable network in which mobile nodes communicate with each other with the help of wireless links without any exact infrastructure. It is a network wherein nodes can act as hosts as well as routers. MANETs may be implemented in military, rescue systems and so forth. and are broadly used. There are many protection troubles related to MANETs because of its dynamic topology, energy constraint of cell nodes and so on. Which make safety of these networks an important research location. MANETs are at risk of many attacks like Wormhole attack, Blackhole attack and Jellyfish attack. Jellyfish attack is DOS attack that's tough to hit upon because it obeys all of the protocol rules. Main focus is on jellyfish attack and its detection and prevention techniques [9].

Apoorva Chandra et al. [2015] this paper simulates and assesses the general execution of zone routing protocol (ZRP), hybrid wireless mesh protocol (HWMP) and ad hoc on demand for distance vector protocol (AODV) against black hole, grey hole and jellyfish reordering attacks which contrarily inversely affect the capability of protocols. Inspite of the fact that for MANET a few protocols and improvised algorithms has never been tried against each unique on various network layer attacks. The overall performance assessment done has quantitatively represented facts for use of specific routing

protocol. For speedy and secure transmission of data for network situation those protocols are used who gather structural alternate of network scenario.
Mobile nodes are open to security attacks as due to their changing network structure and open communication channel. This paper simulated protocols which are being used these days through cell gadgets and based on studies of proactive, reactive and hybrid protocols and the behavior. They exhibit in particular node structure against the vulnerabilities which they exhibit [10].

Sakshi Garg, et al. [2014] this paper discusses an more enhanced AODV routing protocol as a way for defense against Jelly Fish (JF) Delay Variance attack in MANET. The JF put off change attack presents place off in sending the packets at network layer. It uses MAC addresses to calculate the path for forwarding the packets to destination. The attacker node makes delay in sending the packets, which builds end-to-end delay and decreases throughput of the network. Hence the execution of network diminishes widely. We propose an enhancement in AODV protocol so that it will locate the malicious nodes in a network and to dispose of them from the routing direction without their knowledge [11].

VI. Proposed Work

In existing work, they find a jellyfish attacker by calculating the trust value of each node by monitoring every node. But it is not an efficient method to detect an attacker as they can also behave as a valid node in the network.

In our proposed work, we are using the reputation value of each node by fetching its record from the entire neighbour. Now we form the clusters then their cluster head. This process eliminates the communication to the entire network and simplifies the process. In this, we get reputation value by using an indirect method to reduce false acquisition from the node which can be done by malicious node. We make them blacklisted node if the reputation value is less than the threshold value or it was JF attacker. If we found that the node has good reputation then we then used the direct method to calculate trust value to make confirmation that the node is valid. Then update the routing entries to make sure that in future these nodes will not take part in communication. This makes the network more efficient and at ease from attackers.

Proposed Algorithm

```
Step:1   Initialize the network
Step:2   Select one source node S
Step:3   Cluster formation performed
Step:4   Select Cluster head of each cluster then perform further process
Step:5   Flood RREQ for reputation value RV of neighbours
Step:6   If RV > threshold
         Calculate trust value TV
         Else
         Then make them blacklisted
Step:7   If TV > threshold
         Then it is valid
         Else
         Make them blacklisted for a certain period
Step:8   Update the table
Step:9   Send the data through trusted nodes
Step:10  Exit
```

VII. Result Analysis

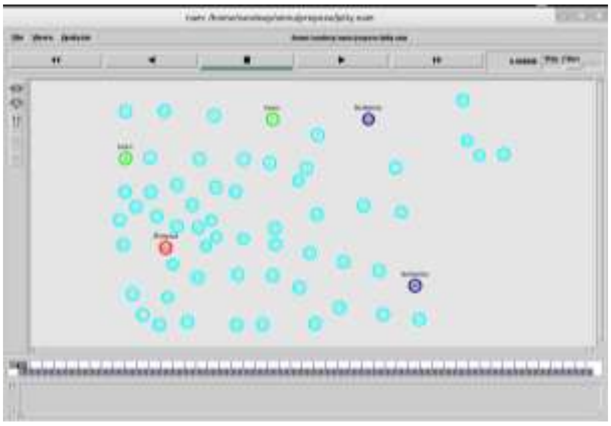

Fig 4. Initialization of network

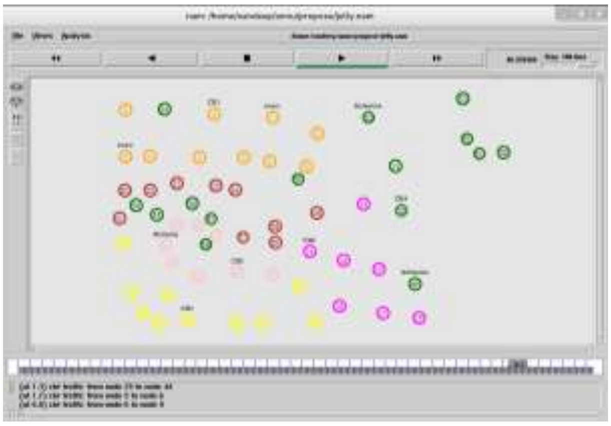

Fig 5. Communication end

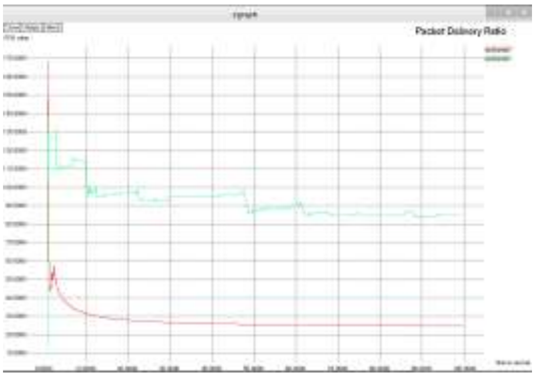

Fig 6. PDR Graph

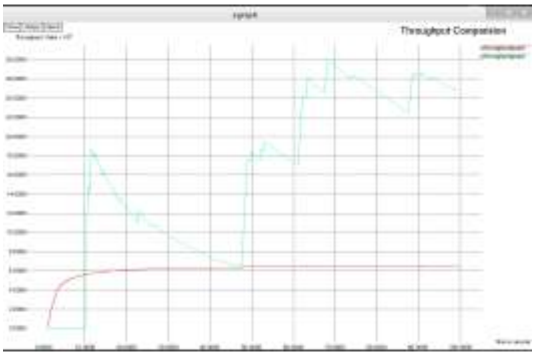

Fig 7. Throughput Graph

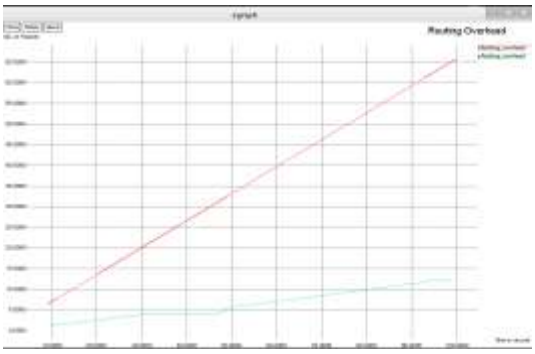

Fig 8. Routing Overhead Graph

CONCLUSION

Jellyfish attack is one of the severe routing attacks amongst all the network layer attacks initiated on MANET. Reputation value is taken from the table which is used to calculate the trust value of each node to eliminate the attackers from the network. A scheme is proposed to detect and prevent JF attacker node from deteriorating the network and effectiveness of scheme. It is evaluated on simulator and results of simulations prove that our proposed algorithm improves the network performance. By this technique we improved the performance of the network and security among the nodes.

REFERENCES

[1] E. Sam Prabhakar and Mr. K. Srinivasan "An efficient detection and countermeasure of a jellyfish attack using dmpd algorithm in MANET" International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 21 Issue 4 – APRIL 2016.

[2] Mr. Ankit M Vaghela, Prof. Mayank Gour, Prof. Ashish Patel "Survey on Delay Based Jellyfish Attack" 2017 IJEDR | Volume 5, Issue 2 | ISSN: 2321-9939, International Journal of Engineering Development and Research.

[3] Agarwal, Pallavi. (2016). Enhance the Security by using Hashing Technique and Trust Values in Vehicular Ad Hoc Networks. International Journal for Science and Advance Research in Technology (IJSART). 2. 78-83.

[4] Ashima Batra , Abhishek Shukla , Sanjeev Thakur , Rana Majumdar "Survey of Routing Protocols for Mobile Ad hoc Networks" IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727 Volume 8, Issue 1 (Nov-Dec. 2012), PP 34-40.

[5] Agarwal, P. and Bhardwaj, N., 2016. Overview of Trust Management in VANET and Various Cryptography Fundamentals. International Journal of Future Generation Communication and Networking, 9(6), pp.137-144.

[6] R.Priyanka , P.Ramkumar "Trust based detection algorithm to mitigate the attacker nodes in MANET"2016 IEEE.

[7] Anjani Garg, Sunil Kumar and Kamlesh Dutta "An Analytical Survey of State of the Art JellyFish Attack Detection and Prevention Techniques"2016 IEEE.

[8] Sakshi Sachdeva, Parneet Kaur "Detection and Analysis of Jellyfish Attack in MANETs" 2016 IEEE.

[9] Simranpreet Kaur, Rupinderdeep kaur and A.K. Verma "Jellyfish attack in MANETs: A Review" 978-1-4799-6085-9/15/$31.00 ©2015 IEEE.

[10] Apoorva Chandra, Sanjeev Thakur "Performance Evaluation of Hybrid Routing Protocols Against Network Layer Attacks in MANET" 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015

[11] Sakshi Garg, Satish Chand "Enhanced AODV protocol for defence against JellyFish Attack on MANETs" 978-1-4799-3080-7114/$31.00 ©2014 IEEE.